

 <p><b>HAWAII HEALTH SYSTEMS</b> CORPORATION <i>"Touching Lives Everyday"</i></p> <p><b>Policy</b></p>	<b>Department:</b> Information Technology Department	<b>Policy No.:</b> <b>ITD 0003</b>
	<b>Issued by:</b> Dennis Sato VP & CIO	<b>Revision No.:</b> None
<b>Subject:</b> <b>Security Incident Response Policy</b>	<b>Approved by:</b>  Thomas M. Driskill, Jr. President & CEO	<b>Effective Date:</b> 07/27/01
		<b>Supersedes Policy:</b> None
		<b>Page:</b> 1 of 2

## I. Purpose

The purpose of this policy is to provide a structure for responding to computer system security incidents in a timely and controlled manner.

## II. Policy

Computer Security Incident Response Teams (CSIRTs) will be created to provide HHSC with a focal point for reporting computer system security incidents and intrusions (attempted or real), and to engage in a coordinated response to these incidents. CSIRTs will report to the Corporate Information Security Officer (CISO). There will be one team supporting each region. Each regional team will be composed of one or more individuals, depending on the user population size at each region. It will be the duty of the CSIRTs to respond to, take appropriate action, and provide reports in the event of a breach in confidentiality, integrity, or availability of any computing resource within their region. One or more individuals from the Corporate Computer Center (CCC) and the Computer Data Center (CDC) will be appointed to serve as the CSIRTs for these facilities. The CCC CSIRT will also assume CSIRT responsibilities for Corporate users.

The CISO will implement and maintain standard formal, documented procedures, for the reporting and response to security breaches. The CISO will ensure that these procedures are adhered to by all CSIRTs within HHSC.

If active intrusion attempts are detected, CSIRTs will be empowered to take immediate action to control the situation. The CISO will be notified immediately after an intrusion attempt has been brought under control.

## III. Definitions

**Incident:** A security incident is any real or suspected adverse event related to the security of telecommunications and computer information systems.

Event: An action directed at a target that is intended to result in a change of state of the target.

Intrusion: Any intentional event where an intruder gains access that compromises the confidentiality, integrity, or availability of computers, networks, or the data residing on them.

#### **IV. REFERENCES/RELATED POLICIES**

Security Management Process

Data Classification Policy

#### **V. POLICY DEVELOPMENT**

**DEVELOPER:** HHIC Policy Committee  
Taylor Summers  
Miles Sato

#### **VI. POLICY APPROVAL**

IT Steering Committee June 13, 2001